tufin The Security Policy Company.

WHERE NETWORK SECURITY MEETS THE CLOUD

6 Ways the Cloud Changes Everything About Enterprise Network Security.

Introduction

Progress is impossible without change. The advent of cloud computing has proven to be one of the most significant changes of this century and has enabled incredible growth — businesses are more productive, cost-efficient, and agile than ever before. According to research from Check Point, over 98% of organizations use some form of cloud-based infrastructure. The cloud has without a doubt become mainstream, mission-critical to business operations today.

However, additional organizational change must occur to safely sustain this rate of innovation. To keep risks in check while supporting the speed of the business, IT has been tasked with extending the same level of control and governance they have over traditional networks into cloud environments. This means **network security (NetSec) teams now have to view their jobs in a fundamentally different way.** In addition to securing the traditional enterprise perimeter, they must also develop a strategy to control access into and across a growing number of hybrid network segments.

This is a significant ask for most network security professionals. Securing a hybrid network is much different than securing a legacy network because critical infrastructure is distributed across a combination of on-prem resources and dynamic, cloud-based services. To reduce risk as much as possible, NetSec needs to adapt to the way security works in the cloud (e.g., using security groups rather than firewalls) and collaborate with other teams to apply security policies consistently across data centers and cloud environments.

Six ways the cloud changes everything about enterprise network security

To become a truly agile enterprise — one that can deliver applications and services at the speed of the cloud without compromising on security — there are several obstacles that must be overcome. Core challenges of practicing effective security policy management and governance across the hybrid network include:

- Fundamental differences in technology and implementation.
- Streamlining connectivity and security across cloud(s) and on-prem networks.
- Proliferation in the number and types of security solutions on the market.
- Siloed or misaligned teams involved in the management of hybrid security.
- Business expectation of increased speed and agility.

It can be difficult to overcome these challenges without fully understanding how different the cloud is compared to traditional networks. Additionally, without a way to centrally manage the hybrid architecture, there is a higher likelihood of mistakes and configuration drift between cloud and legacy policies.

Let's take a look at six ways in which the cloud changes everything about enterprise network security, along with guidance on how to adapt.

tufin

1 Network security in the cloud is more piecemeal

Traditional enterprise network security comes with a level of comfort because there is an established toolkit for the task at hand. NetSec teams are deeply familiar with solutions such as traditional firewalls and next-gen firewalls (NGFWs), along with architectural approaches like network segmentation and zoning.

As enterprises continue to move applications to public and private cloud instances, they are adopting new cloud service providers such as AWS, Azure, and Google Cloud Platform, each with its own platform-specific security framework. This places a significant burden on NetSec teams because they are being asked to design and enforce consistent security policy across these divergent platforms despite the fact that they are not cloud technology experts.

Without unified visibility, NetSec is forced to use a plethora of tools and check multiple consoles just to gain a vague picture of whether or not security mechanisms — like firewalls, security groups, infrastructure as code, and microsegments — are working properly together. **Inability to see the entire hybrid network and associated controls will inevitably lead to issues** such as blind spots, slow mean time to repair (MTTR), and false positives.

For example, let's say an asset with cloud access to an enterprise resource contains a vulnerability and a security alert is issued; however, there is actually a firewall along the way that provides protection so the alert is not a top priority. This increased noise can distract teams from identifying and responding to real security concerns. When hundreds or thousands of security alerts are being issued every day, it is critical for NetSec to be able to accurately assess risk and prioritize remediation efforts based on the organization's unique situation.

Tufin gives NetSec teams the ability to centralize visibility and manage security policies for the entire hybrid network. Key features include:

Topology intelligence:
A comprehensive network topology map for path analysis and troubleshooting.

Unified Security Policy (USP):
A single place to design and manage requirements for governing segments and traffic across your hybrid network.

> **"The main drivers [to adopt Tufin] were to increase automation and visibility into the network and firewall topology. Ultimately, we wanted to accelerate the delivery of firewall requests. We wanted to deliver faster."**
>
> – Network security lead, financial services company

tufin

2 Everything moves faster in the cloud

The cloud has sped up virtually everything in IT — technology adoption, infrastructure change, application deployment, and more. This comes as a delight to developers and executives who want to accelerate the deployment of revenue-generating applications.

NetSec, on the other hand, is often overwhelmed by this breakneck pace of change. Rapid provisioning and scalability of resources means they are left struggling to secure dynamic workloads as everything in the cloud is constantly scaling up and down. Every day network teams are inundated with requests from application owners who want to connect their applications to additional services. To do this effectively NetSec must be able to answer:

- Where does the application reside?
- What is the underlying infrastructure?
- Does the requester have sufficient permissions?
- Which policies govern this application's connectivity?

The only way to keep up with the fast pace of connection requests and accurately evaluate associated risk is through intelligent automation. Relying on the same manual processes (like spreadsheets, email, and ad hoc research) carries a high probability of human error that can lead to network-related outages and application downtime. In fact, a recent survey from Uptime Institute discovered that human error plays a role in 67%-80% of all outages.

Tufin provides a common language that allows teams to practice dynamic security policy management and evaluate changes to prevent undue risk from being introduced. Key features include:

Access and connectivity risk analysis: Automatically identifies high-risk configurations and analyzes them against industry benchmarks and regulatory requirements.

Proactive change management: Real-time visibility and automatic risk identification for every proposed network or cloud change and its impact on security posture.

Full ITSM integration: Seamlessly triggers change design workflows (access requests, group modification, rule recertification, etc.) as soon as tickets are opened.

"The top benefit we've experienced with Tufin is speed, which means that we fit into the company's agile vision. If they want to deploy any application, all they have to do is access Tufin and make a request. Then, we can implement it in hours instead of weeks."

– Technical lead for security, financial services company

tufin

3 The cloud demands a higher degree of collaboration between NetSec and application teams

In traditional network environments, if a user wants to connect A to B they have to go through NetSec by default. This is not always the case in hybrid networks, where security teams give up a great deal of control in the name of agility and faster application delivery.

Let's say an application developer submits a request to spin up a new cloud server. The DevOps or CloudOps team then provisions the server, attaches a security group with overly permissive access rules, and the developers move forward with their project. NetSec may not even know this occurred — if the process took place outside of their scope, they lack tools that provide an adequate level of awareness. In increasingly common hybrid and multi-cloud environments, it is virtually impossible for NetSec to achieve unified cross-platform and multi-vendor visibility.

Of course, this security gap doesn't come from a place of maliciousness or intentional negligence. **Application teams do care about security but are typically not trained in the discipline or measured on security performance.** They are measured on how fast they can get code out the door, often lacking the tools and training to assess the security of the code they are writing or its impact on the business.

Tufin facilitates necessary collaboration between NetSec and developers while enabling faster, safer application delivery. Key features include:

DevOps automation:
Defines a policy framework and deploys context-specific controls into developers' workflows without endless security reviews that slow down deployment.

CI/CD integration:
Ensures applications adhere to security policy with built-in policy checks that flag violations well before code deployment.

Security guardrails:
Prevent network misconfigurations and connectivity errors that would expose sensitive data to the internet.

> **"We can deploy the applications more quickly to the customers and they will work on all of the systems and buildup will be faster. We have a clear process, transparency on what's going on, and can verify quality when something goes wrong."**
>
> – Product owner of security orchestration, telecommunications company

tufin

4 Continuous validation of infrastructure as code is now a security requirement

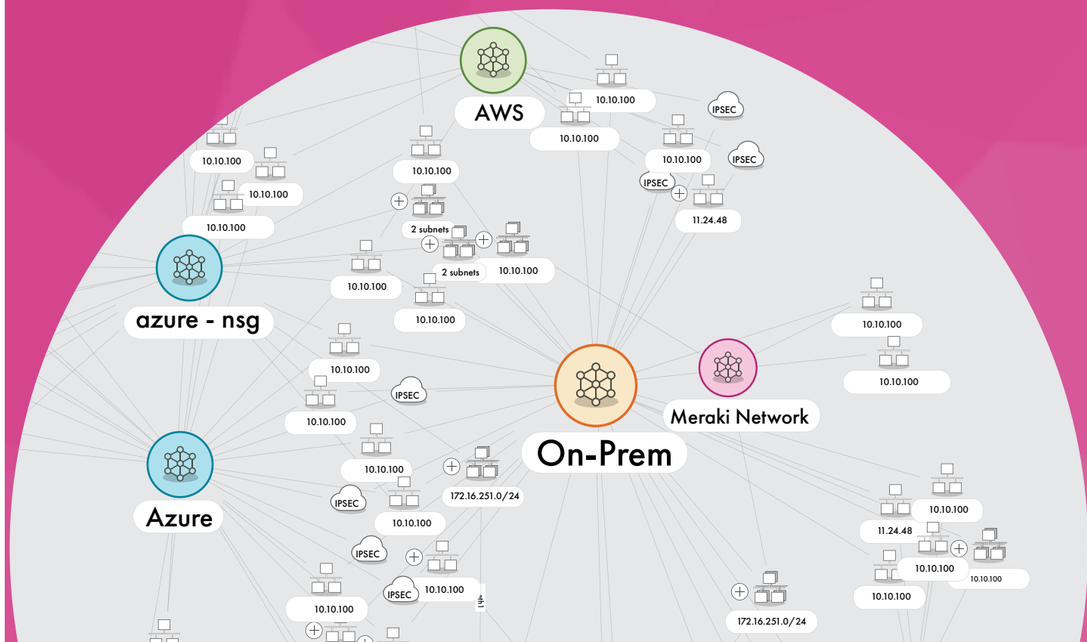
Infrastructure as code (IaC) — the process of provisioning and managing resources in the cloud using machine-readable definition files that describe how and where configurations are deployed — is foundational to development and cloud operations agility. While IaC enables key benefits such as speed, standardization, and effective version control, it also introduces security concerns.

The core conundrum of IaC security is that the people who read/write code often don't have deep cybersecurity knowledge and the people who have deep security knowledge often don't know how to read/write code. **Miscommunication and lack of IaC security alignment can lead to the deployment of cloud misconfigurations at scale**, resulting in deployment failures, data breaches and/or application outages. It's a contributing factor to Gartner's prediction that through 2025, 99% of cloud security failures will be the customer's fault, not the service provider's.

Tufin helps application teams verify proper IaC security during the development phase, mitigating risk and significantly reducing the time and effort required to confirm the security of cloud deployments. Key features include:

Continuous compliance automation: Scans build files to identify policy violations and highlight which specific areas need to be reconfigured.

IaC platform integration: Automatically analyzes the security impact of proposed changes before implementing them in cloud infrastructure.



tufin

5 Misconfigurations run rampant in the cloud

Misconfigurations are the biggest cause of security breaches in the cloud, bar none, as they introduce vulnerabilities that can be exploited by threat actors. The National Security Agency has even pointed to misconfigurations as the number one threat to cloud security.

Misconfigurations are very frequently a result of lack of effective security policy management in the cloud. This is yet another area in which the highly fluid and rapidly expanding nature of the cloud makes keeping up with relevant changes difficult. A survey from Fugue found that lack of awareness of cloud security and policies is the most cited reason for misconfigurations.

That being said, it's important to keep in mind that having a risk or vulnerability doesn't automatically mean it can be exploited. **It's the combination of vulnerabilities and connectivity to critical assets that results in exploitability** and thus should be addressed ASAP. A vulnerable system that is isolated from the internet, for instance, is not a prioritized risk.

Tufin gives network and cloud teams the ability to better see and understand connectivity among systems in a hybrid network so they can proactively remediate security policy violations. Key features include:

Misconfiguration detection:
Automatically surfaces misconfigurations, such as rule permissiveness and shadowing, and issues real-time alerts.

Vulnerability scanner integration:
Prioritizes remediation and mitigation efforts by complementing vulnerability scanner data with network connectivity insights to determine exploitability.

Application-centric topology:
Displays all deployed assets, configurations, and security settings to ensure only trusted workloads and traffic are allowed.

Tufin reduces the risk of a vulnerability-related breach by 80%.

*Source: The Total Economic Impact™ of Tufin

tufin

6 Compliance in the cloud is more complex

Most cloud service providers practice the shared responsibility model in which the provider is accountable for securing the cloud infrastructure and the customer is in charge of protecting their data and assets. There is a common misconception that this model makes security compliance in the cloud much easier compared to traditional networks.

While it's true that achieving compliance in a cloud-only setup should be less burdensome in theory, the majority of enterprises are dealing with hybrid and multi-cloud environments. Lack of centralized visibility across these complex, fragmented networks makes it difficult to achieve continuous compliance and audit readiness for applicable regulations.

For example, if a business must follow the Health Insurance Portability and Accountability Act (HIPAA), they are required to know where any protected health information (PHI) data is being stored, moved, or accessed. This requires a tremendous amount of manual effort to constantly analyze the compliance of security controls across physical networks and cloud environments.

NetSec, specifically, must constantly be prepared to answer questions related to:

- Configurations: How did you configure your security posture?
- Segmentation: How is the network segmented based on the nature of the data?
- Process: Is everything thoroughly documented and audit-ready?
- Reporting: Are you able to demonstrate the current state of controls and report on it?

Enterprises today have more business units, developer teams, and third parties than ever before. Plus, in increasingly common growth scenarios such as mergers and acquisitions (M&A), a new company must be quickly added to the hybrid network, introducing a legion of potential compliance and security risks. Keeping up with this complexity and growing risk in rapidly changing hybrid networks is truly impossible without automated assistance.

Tufin helps application teams verify proper IaC security during the development phase, mitigating risk and significantly reducing the time and effort required to confirm the security of cloud deployments. Key features include:

Unified Security Policy: Single pane of glass that displays all rules that are applied across the hybrid network and which adhere to or violate policy.

Continuous compliance automation: Built-in proactive risk analysis of changes across firewalls, routers, switches, SDNs, public clouds, and containers to ensure connectivity.

Audit trail: Automatically generates a variety of customizable audit reports that comply with regulatory standards such as PCI DSS, SOX, NERC CIP, and more.

> **"Tufin has enabled us to achieve continuous compliance with PCI DSS for our Cisco and Check Point firewalls and to cut audit preparation time in half."**
>
> – Laurent Klefstad, Leader for Systems, Network, and Telecom at Monext

tufin

Time to change for the better

Enterprises must accept that change is needed to help network security enable rapid progress across the business while increasing security and agility. Rather than go it alone, these stretched-thin teams deserve a new toolkit to help them adapt to new ways of working in the cloud.

Tufin is the answer. Our platform offers unified, end-to-end network visibility and unparalleled security automation across network and cloud environments. With the power of Tufin, your teams will be able to deploy apps faster, remediate issues more quickly, maximize efficiency, and stay audit-ready year round.

To hear directly from our customers and see how Tufin delivers a 144% ROI, download The Total Economic Impact™ of Tufin report.